Secure Network Tri-Lab User Access

In the secure restricted network, the three Laboratories (SNL, LLNL, and LANL) have established a high speed Wide Area Network (WAN) through the DisCom project. This allows logins and file transfers at reasonable speeds between the secure clusters such as ASC Purple at LLNL, File Transfer Agents (FTAs) at LANL, and ASC Redstorm at SNL.

NOTE: there is no equivalent WAN in the **open** network (Unclassified Protected, or Yellow network). Logins and file transfers between systems such as Up at LLNL and Flash at LANL must go through both Laboratory firewalls and across the Internet using standard tools such as ssh and scp with VPN.

You can find HPC documentation and information for LLNL and SNL with a common URL: http://hpc.*site*.gov, where "site" is one of llnl, sandia, or lanl. Here are the links to Livermore, and to Sandia. Also, the main documentation page for computing at Livermore is here: https://computing.llnl.gov/.

Logging-in from LANL to LLNL

1. **Get a Kerberos Ticket**.
   From a LANL ICN system, issue two commands: `k5destroy` and `k5init -f`.

   In order to reach LLNL, you must have a valid LANL kerberos ticket with a LANL IP address, **and** an active account at LLNL (see the Getting an Account web page to obtain one). Typically, you will start from a gateway system in the ICN because of filesystem access. For example, red-fta8.lanl.gov and vm000.lanl.gov will allow a direct ssh into the LLNL Purple cluster.

   Upon logging-in to an ICN cluster such as red-fta5 via ssh, you may already have a kerberos ticket forwarded from your desktop. However, that ticket probably does **not** have the correct properties. Issue the `kinit -f` command to obtain a new one. Provide a passcode from your CryptoCard when it prompts you.

   Note: kerberos tickets expire, so verify that you have a valid ticket with the `klist` command. Also, LLNL has switched to ssh protocol 2, so there is no need for the -1 option to the ssh command.

2. **Connect to LLNL**.
   From a LANL ICN front-end node use the `ssh` command:
   `ssh -l LLNLmoniker ascpurple1.llnl.gov`
   or
   `ssh -l LLNLmoniker ascpurple2.llnl.gov`
   or
   `ssh -l LLNLmoniker ascpurple3.llnl.gov`
   or
   `ssh -l LLNLmoniker ascpurple4.llnl.gov`

   - This connects correctly to purple, but does not forward your kerberos ticket to LLNL. You may need to obtain a new ticket there after logging-in.
   - Note that you must provide your LLNL moniker (username) with the -l option (lower case L) if it is not the same as your LANL moniker.
   - add `-X` to the ssh command line if you want X11 forwarding. This allows you to run Xwindow commands such as TotalView, emacs, xterm, etc. and display them back to your desktop. This is a necessary but not sufficient piece of establishing your X11 connection. The other pieces include opening-up your desktop client (via xauth or xhost) and setting your DISPLAY environment variable within your shell on the server, purple. **Caution:** the xhost command opens a security vulnerability on your client workstation.

   Alternative: From your workstation, you can use your fully qualified LANL moniker to reach purple with your secure LANL Cryptocard:

   ```
   ssh -l LANLmoniker@lanl.gov ascpurple4.llnl.gov
   ```

   This will ask you for a passcode, and you can provide one with your secure LANL Cryptocard.

3. (Optional) If you need to acquire a kerberos ticket on purple, issue the
`/usr/local/krb5/bin/kinit LANLmoniker@lanl.gov`
command. This full path is important, if you don't specify it you will get the wrong kinit. You only need to do this step if you want to run something that requires a ticket, like pftp. Use your LANL moniker in this command, and then use your LANL cryptocard when requested.

Logging-in from LANL to SNL's redstorm-s

1. First obtain a valid kerberos ticket in your LANL shell session. To reach redstorm-s, you must have a valid kerberos ticket with an IP address. Usually, this means that you need to start from red-fta6.lanl.gov - in most cases you cannot reach SNL from your desktop. Upon first logging-in to our FTA, you will probably have a kerberos ticket already. If not, you can issue the `kinit -f` command to obtain one. Provide a passcode from your CryptoCard when it asks for a password.
Note: kerberos tickets expire, so verify that you have a valid ticket with the `klist` command.

2. `ssh [-l SNLmoniker | -l LANLmoniker@lanl.gov] redstorm-s.sandia.gov`
In this command, use either your LANL moniker qualified by the LANL domain for the argument to the -l (lower case L) option, or use your Sandia moniker.
Note: since Redstorm is running ssh protocol 2, your kerberos ticket should forward with no problems.

Logging-in from LLNL's purple to the LANL FTA gateways

1. First obtain a valid kerberos ticket in the LLNL domain. Usually you accomplish this via a `/usr/local/krb5/bin/kinit` command.

2. `ssh -l LANLmoniker red-fta9.lanl.gov`
You must use the -l (lower case L) moniker, even if your monikers are the same in both places. This is a known bug that we are working on.

Logging-in from SNL's Redstorm to the LANL FTA gateways

1. First acquire a valid Sandia DCE kerberos ticket. You can do so by running the following two commands (insert your moniker and your Lab domain).
`setenv KRB5CCNAME /tmp/krb5cc_yourmoniker`
`kinit yourmoniker@dce.yourlab.gov`

2. from redstorm: `ssh red-fta7.lanl.gov`
from sasn101: `ssh -c3des red-fta9.lanl.gov`

File Transfer

One of the important issues for Tri-Lab access of the ASCI systems is file transfer in-between the sites and Laboratories. We have written several scripts to simplify parallel transfers to/from the secure Tri-Lab HPC clusters across the Wide Area Network (WAN). This is a secure encrypted network supporting high bandwidth between the individual ASCI machines (Purple, Redstorm, red-ftaN, HPSS, etc.). You can use these special scripts to transfer files over the secure DisCom WAN; here is how:

1. If you are on a secure LANL front-end system (lc-3, red-fta5, etc.), log-in to a compute resource using the `llogin` command.

2. Set your KRB5CCNAME environment variable. Example in tcsh/csh for username "abc":
`setenv KRB5CCNAME /tmp/krb5cc_abc`

This is important if you see an error such as "k5init: No credentials cache file found when initializing cache".

3. Obtain a Kerberos Ticket

   The general syntax to obtain a ticket is through the `kinit yourmoniker@yourdomain` command. LANL users run the `kinit` command, and on the LLNL systems, LANL users run the `/usr/local/krb5/bin/kinit` command.

   Example for LANL user "abc" on the LANL red-fta8 system:
   `kinit abc@lanl.gov`
   Example for LLNL user "xyz" who connects from LLNL with DCE kerberos ticket:
   `kinit xyz@dce.llnl.gov`
   Example for LANL user "abc" on the ascipurple cluster:
   `/usr/local/krb5/bin/kinit abc@lanl.gov`

   LANL users take note: if you have a forwarded kerberos ticket on a red-ftaN, you still need to run a `kinit` command on the FTA or a `/usr/local/krb5/bin/kinit` on ascipurple since you need one with an address.

4. Use the parallel ftp (pftp) command scripts in /usr/local/bin. You can see them with an
   `ls /usr/local/bin/pftp*`
   command. The pftp commands ship files to specific systems (janus, llnl, etc.). As an example, here is the command for transferring a file to the LLNL HPSS:
   `pftp2llnl filename`

5. **Note**: Sandia redstorm-s and redrose-s users have a custom command, `multi2lanl`, that automatically transfers files over the high-speed DisCom WAN to the LANL HPSS. It is a wrapper script that runs ftp. To use it, simply type `multi2lanl` from a shell on the Sandia platform, and it will give you a prompt after authenticating. It may ask for a passcode, and you can use your LANL Red (Secure Restricted) Network cryptocard. Then you can issue your `get` and `put` commands between the local filesystem and the LANL HPSS in the Red Network. At this writing, `multi2lanl` does not seem to accept any batch style commands.

ASC Purple Cluster

Getting an Account

Sarape is the link for accounts ASC systems in general. It's useful to know that DCE User Name means moniker, without the @lanl.gov appended. Purple account approvals are currently handled by the Purple ASC Level 1 Milepost lead, but access is granted (with warnings) in most cases.

Warnings

LLNL is undertaking a rolling replacement of nearly all disks in the GPFS scratch file system. Until that process is complete, the file system for Purple is undersized and purging is in effect. LLNL is also recommending data checking (checksums), and there have been issues recognized with accessing small memory page sizes by default. Once you have an account, more detail is available in the news items on Purple upon login.

Getting Cycles:

Access to major compute cycles on the ASC Purple Capability Computing platform will be via a new Capability Computing Campaign (CCC) selection process. For details, see CCC_Call.doc. Generally, a handful of computing campaigns culminating in one or more capability (more than half the processors utilized) runs will be priority-selected across the ASC complex and given all compute cycles for roughly a six-month timeframe. Other users may submit jobs in a fairshare-based preemptable standby queue for computational progress as idle time in the capability campaigns permits.

Information:

LLNL has provided a draft Purple Computation Environment document detailing policies and procedures for effective use of the Purple platform. Additionally, there is a Good Citizenship document, an online tutorial, and a general Purple website at LLNL.

ASC Red Storm Cluster

On this page, we will provide links to Sandia National Laboratory web pages that describe user access, environment, architecture, etc. of the new Red Storm cluster from Cray, Inc.

Getting an Account

Sarape is the link for accounts on Sandia systems in general. It's useful to know that DCE User Name means moniker, without the @lanl.gov appended. Red Storm account approvals are being handled by the Integrated Computing program lead, and remain restricted.

Information:

The Red Storm Fact Sheet and Red Storm Usage Model are available for download in pdf format. The former is a quick press-release style overview of the Red Storm system, while the latter contains a wealth of information about the projected state of Red Storm in the FY05 timeframe. The Usage Model also contains an appendix which lists the tri-lab ACE user requirements and documents which ones Red Storm will provide and which it will not.

Sandia web pages include the Red Storm Web Page and the CLIK database at Sandia. The database is a repository of web pages and user- and admin-generated knowledge base articles relevant to Red Storm. To log in to the main Red Storm page or to search the CLIK database, LANL users must log in with <lanlmoniker@lanl.gov> and a cryptocard password. CLIK gives access to web pages not otherwise accessible from LANL desktops. Please note that at this time some CLIK search results still are inaccessible; Sandia is working on this issue.

Schedule:

The Red Storm platform is now in limited availability mode, meaning that approved users can use the machine. The number of approved (by the Advanced Applications program) users remains small for the time being.

Classified Access

Early access note: For now, use the specific login node rslogin01s.sandia.gov in place of the round-robin server redstorm-s.sandia.gov in the instructions below.

Logging In

Login to the classified partition is fairly straightforward, though most users must connect via one of LANL's supercomputer front ends (see **A Note about Desktop Access**, below). To reach Red Storm, run

```
ssh qfe2.lanl.gov
kinit
ssh -l <lanlmoniker@lanl.gov> redstorm-s.sandia.gov
```

Data Transfer

Transferring files to or from Red Storm on the classified network is available via scp. To transfer something to your home directory on Red Storm from a LANL system, and with a LANL kerberos ticket, run

```
scp -o "User=<lanlmoniker@lanl.gov>" /mypath/myfile redstorm-s.sandia.gov:/home/<snlmoniker>/
```

To transfer larger files via the DisCom WAN use one of the pftp2... commands found in /usr/local/bin, as in

```
pftp2qb
```

and proceed interactively.

A Note about Desktop Access: Only specific user LANs at Los Alamos are permitted to connect directly to external sites like Red Storm. If your LAN is not one of these and you would like to connect from your desktop, see your LAN administrator. The administrator must receive approval from LANL's Secure ICN ISSO for systems on the LAN to connect externally. They proabably also need to change your default krb5.conf so that the standard kerberos ticket granted at login (1) has addresses and (2) is not proxiable. The LAN administrator may contact consult@lanl.gov for details.

Unclassified (Yellow) Access

Logging In

At Sandia, the equivalent network to our Yellow (Unclassified Protected) Network is the "Black" network, otherwise known as the Sandia Restricted Network (SRN). You need your Sandia Cryptocard to access their Black network, and you will also need your LANL cryptocard for authentication. To get your SNL passcode from the Cryptocard:

1. press the password button to turn it on
2. enter your pin
3. press `ent` and you will see your moniker/username on the Cryptocard display
4. press `ent` again to see the passcode.

To access the SRN, use this command sequence:

```
ssh -l <lanlmoniker@lanl.gov> srngate.sandia.gov

<many warnings>

lanlmoniker@lanl.gov@srngate.sandia.gov's password: <SNL passcode>

       Welcome Sandia moniker to the ssh gateway

               1 -  telnet session
               2 -  ssh session
               Q -  Quit

    Enter a selection from above: 2

System Name: rslogin10.sandia.gov
Username: <lanlmoniker@lanl.gov>
lanlmoniker@lanl.gov's password:  <LANL passcode>
```

Data Transfer

Transferring files to or from Red Storm in the unclassified network is a two-step process. To transfer data from LANL to SNL, files must first be transferred to SNL's ASC Red platform, then pulled from there to the Red Storm platform. To transfer data from SNL to LANL, data must be pushed from Red Storm to ASC Red, then moved to LANL. The ASC Red/LANL transfer may be initiated from either side, but the ASC Red/Red Storm transfer must be initiated from Red Storm. See the examples below for details.

Moving data from Red Storm to a LANL system:

Login to Red Storm as described above. Once on a Red Storm login node, run

```
scp myfile sasn100:/scratch/<snlmoniker>/myfile
```

From a LANL desktop, with a LANL kerberos ticket, you can then run

```
scp -o "User=<lanlmoniker@lanl.gov>" sasn100.sandia.gov:/scratch/<snlmoniker>/myfile /mypath/myfile
```

Moving data from a LANL system to Red Storm:

From a LANL system, with a LANL kerberos ticket, run

```
scp -o "User=<lanlmoniker@lanl.gov>" myfile sasn100.sandia.gov:/scratch/<snlmoniker>
```

Then log in to Red Storm as described above. Once on a Red Storm login node, run

```
scp sasn100:/scratch/<snlmoniker>/myfile /mypath/myfile
```